

UNCLASSIFIED

Defense Technical Information Center  
Compilation Part Notice

ADP013331

TITLE: Identifying Enterprise Intrusion

DISTRIBUTION: Approved for public release, distribution unlimited  
Availability: Hard copy only.

This paper is part of the following report:

TITLE: Multimedia Visualization of Massive Military Datasets [Atelier  
OTAN sur la visualisation multimedia d'ensembles massifs de donnees  
militaires]

To order the complete compilation report, use: ADA408812

The component part is provided here to allow users access to individually authored sections of proceedings, annals, symposia, etc. However, the component should be considered within the context of the overall compilation report and not as a stand-alone technical report.

The following component part numbers comprise the compilation report:  
ADP013309 thru ADP013341

UNCLASSIFIED

# Identifying Enterprise Intrusion

**A. Miller**

Distinguished Professor of Electrical and Computer Engineering  
University of Missouri-Rolla  
125 Emerson Electric Co. Hall  
Rolla, MO 65409-0040  
United States

*In the interests of readability and understandability, it is RTO policy to publish PowerPoint presentations only when accompanied by supporting text. There are instances however, when the provision of such supporting text is not possible hence at the time of publishing, no accompanying text was available for the following PowerPoint presentation.*

**Click here to view PowerPoint presentation; Press Esc to exit**

## Discussion – Paper 20

Bill Wright—scalability problem, data mining—finding the very few problems that really represent attacks  
Dealing with False positives

MIT Bottleneck ID technique—try to characterize normal information flows of the enterprise, rather than characterize what attack would look like

Objection that still have false positives

Bayesian or neural models to distinguish between what is really unusual and what is normal traffic

Sharing the raw data in intrusion detection not done—trust the partner to perform their part of the interpretation correctly

Taxonomy (Kunar-session chair) problems with large data sets?

Milan—says uses an ontology approach

Seems to be some confusion w.r.t. use of terms “visualisation” vs. “taxonomy” vs. “ontology”

Portals—customized interfaces

Use one window to access all types of information/applications